Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	4445	707/3.ccls.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2004/11/19 14:04
L2	1331	707/6.ccls.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2004/11/19 14:04
L3	1033	707/9.ccls.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2004/11/19 14:04
L4	4246	707/10.ccls.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2004/11/19 14:04
L5	1568	707/101.ccls.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2004/11/19 14:05
L6	1746	707/200.ccls.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2004/11/19 14:05
L7	4833	709/203.ccls.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2004/11/19 14:05
L8	2733	709/219.ccls.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2004/11/19 14:05
L9	2100	709/229.ccls.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2004/11/19 14:05
L10	9	(1 2 3 4 5 6 7 8 9) and (MD5 adj function)	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2004/11/19 14:07
L11	1427	(((file adj name) filename) with function)	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2004/11/19 14:08
L12	39	(((file adj name) filename) with (hash adj function))	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2004/11/19 14:08

L13	1	(((file adj name) filename) with (MD5 adj function))	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2004/11/19 14:09
L14	377	(identifier with ((MD5 hash) adj function))	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2004/11/19 14:12
L15	46	14 and licens$	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2004/11/19 14:09
L16	33	function with (content near (data adj file))	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2004/11/19 14:10
L17	131	truename (true adj name)	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2004/11/19 14:10
L18	40	17 and (@rlad<="19950411" @ad<="19950411")	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2004/11/19 14:18
L19	1657	(1 2 3 4 5 6 7 8 9) and (@rlad<="19950411" @ad<="19950411")	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2004/11/19 14:11
L20	49	19 and ((MD5 hash) adj function)	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2004/11/19 14:12
L21	9	705/50.ccls. and (@rlad<="19950411" @ad<="19950411")	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2004/11/19 14:18
L22	109	705/51.ccls. and (@rlad<="19950411" @ad<="19950411")	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2004/11/19 14:18
L23	64	705/52.ccls. and (@rlad<="19950411" @ad<="19950411")	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2004/11/19 14:19
L24	51	705/59.ccls. and (@rlad<="19950411" @ad<="19950411")	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2004/11/19 14:19

L25	55	(22 23 24) and (hash md5)	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2004/11/19 14:19

Terms used **file name hash MD5**

Found **15** of **145,831**

Sort results by relevance

Display results expanded form

Save results to a Binder

Search Tips

Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 15 of 15

Relevance scale

1 Measurement: A high-level programming environment for packet trace anonymization and transformation

Ruoming Pang, Vern Paxson

August 2003 **Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications**

Full text available: pdf(251.27 KB) Additional Information: full citation, abstract, references, index terms

Packet traces of operational Internet traffic are invaluable to network research, but public sharing of such traces is severely limited by the need to first remove all sensitive information. Current trace anonymization technology leaves only the packet headers intact, completely stripping the contents; to our knowledge, there are no publicly available traces of any significant size that contain packet payloads. We describe a new approach to transform and anonymize packet traces. Our tool provide ...

Keywords: anonymization, internet, measurement, network intrusion detection, packet trace, privacy, transformation

2 Zodiac: a history-based interactive video authoring system

Tzi-cker Chiueh, Tulika Mitra, Anindya Neogi, Chuan-Kai Yang

September 1998 **Proceedings of the sixth ACM international conference on Multimedia**

Full text available: pdf(1.10 MB) Additional Information: full citation, references, citings, index terms

3 Managing routing tables for URL routers in content distribution networks

Zornitza Genova Prodanoff, Kenneth J. Christensen

May 2004 **International Journal of Network Management**, Volume 14 Issue 3

Full text available: pdf(337.00 KB) Additional Information: full citation, abstract, references, index terms

Large-scale content distribution networks (CDNs) can be built using URL routers to redirect client HTTP requests to the nearest content source. URL routers employ very large routing tables. To improve the manageability of CDNs, we propose to use URL signatures to reduce the size of routing tables and aggressive hashing to speed-up routing look-ups.

4 Signature extraction for overlap detection in documents

Raphael A. Finkel, Arkady Zaslavsky, Krisztián Monostori, Heinz Schmidt

January 2002 **Australian Computer Science Communications , Proceedings of the twenty-fifth Australasian conference on Computer science - Volume 4**, Volume 24 Issue 1

Full text available: pdf(715.78 KB) Additional Information: full citation, abstract, references, citings, index terms

Easy access to the Web has led to increased potential for students cheating on assignments by plagiarising others' work. By the same token, Web-based tools offer the potential for instructors to check submitted assignments for signs of plagiarism. Overlap-detection tools are easy to use and accurate in plagiarism detection, so they can be an excellent deterrent to plagiarism. Documents can overlap for other reasons, too: Old documents are superseded, and authors summarize previous work identical ...

Keywords: plagiarism document overlap culling digest

5 The architecture of robust publishing systems

Marc Waldman, Aviel D. Rubin, Lorrie Faith Cranor

November 2001 **ACM Transactions on Internet Technology (TOIT)**, Volume 1 Issue 2

Full text available: pdf(680.21 KB) Additional Information: full citation, abstract, references, index terms

The Internet in its present form does not protect content from censorship. It is straightforward to trace any document back to a specific Web server, and usually directly to an individual. As we discuss below, there are valid reasons for publishing a document in a censorship-resistant manner. Unfortunately, few tools exist that facilitate this form of publishing. We describe the architecture of robust systems for publishing content on the Web. The discussion is in the context of Publius, as that ...

Keywords: Censorship resistance, Web publishing

6 Incremental cryptography and application to virus protection

Mihir Bellare, Oded Goldreich, Shafi Goldwasser

May 1995 **Proceedings of the twenty-seventh annual ACM symposium on Theory of computing**

Full text available: pdf(1.65 MB) Additional Information: full citation, references, citings, index terms

7 Using content-derived names for configuration management

Jeffrey K. Hollingsworth, Ethan L. Miller

May 1997 **ACM SIGSOFT Software Engineering Notes , Proceedings of the 1997 symposium on Software reusability**, Volume 22 Issue 3

Full text available: pdf(753.19 KB) Additional Information: full citation, references, citings, index terms

8 Interposed request routing for scalable network storage

February 2002 **ACM Transactions on Computer Systems (TOCS)**, Volume 20 Issue 1

Full text available: pdf(363.12 KB) Additional Information: full citation, abstract, references, index terms, review

This paper explores interposed request routing in Slice, a new storage system architecture for high-speed networks incorporating network-attached block storage. Slice interposes a request switching filter---called a μ*proxy*---along each client's network path to the storage service (e.g., in a network adapter or switch). The μproxy intercepts request traffic and distributes it across a server ensemble. We propose request routing schemes for I/O and file service traffic, and explore th ...

Keywords: Content switch, file server, network file system, network storage, request redirection, service virtualization

9 Separating key management from file system security

David Mazières, Michael Kaminsky, M. Frans Kaashoek, Emmett Witchel

December 1999 **ACM SIGOPS Operating Systems Review , Proceedings of the seventeenth ACM symposium on Operating systems principles**, Volume 33

Issue 5

Full text available: pdf(1.77 MB) Additional Information: full citation, abstract, references, citings, index terms

No secure network file system has ever grown to span the Internet. Existing systems all lack adequate key management for security at a global scale. Given the diversity of the Internet, any particular mechanism a file system employs to manage keys will fail to support many types of use.We propose separating key management from file system security, letting the world share a single global file system no matter how individuals manage keys. We present SFS, a secure file system that avoids internal ...

10 Dynamic services and analysis: Make it fresh, make it quick: searching a network of personal webservers

Mayank Bawa, Roberto J. Bayardo, Sridhar Rajagopalan, Eugene J. Shekita

May 2003 **Proceedings of the twelfth international conference on World Wide Web**

Full text available: pdf(500.28 KB) Additional Information: full citation, abstract, references, citings, index terms

Personal webservers have proven to be a popular means of sharing files and peer collaboration. Unfortunately, the transient availability and rapidly evolving content on such hosts render centralized, crawl-based search indices stale and incomplete. To address this problem, we propose YouSearch, a distributed search application for personal webservers operating within a shared context (e.g., a corporate intranet). With YouSearch, search results are always fast, fresh and complete -- properties we ...

Keywords: P2P, decentralized systems, information communities, intranet search, peer-to-peer networks, web search

11 Location-independent naming for virtual distributed software repositories

Shirley Browne, Jack Dongarra, Stan Green, Keith Moore, Theresa Pepin, Tom Rowan, Reed Wade

August 1995 **ACM SIGSOFT Software Engineering Notes , Proceedings of the 1995 Symposium on Software reusability**, Volume 20 Issue SI

Full text available: pdf(894.55 KB) Additional Information: full citation, abstract, references, citings, index terms

A location-independent naming system for network resources has been designed to facilitate organization and description of software components accessible through a virtual distributed repository. This naming system enables easy and efficient searching and retrieval, and it addresses many of the consistency, authenticity, and integrity issues involved with distributed software repositories by providing mechanisms for grouping resources and for authenticity and integrity checking. This paper ...

12 Access Control Models and Mechanisms: Cryptographic access control in a distributed file system

Anthony Harrington, Christian Jensen

June 2003 **Proceedings of the eighth ACM symposium on Access control models and technologies**

Full text available: pdf(249.24 KB) Additional Information: full citation, abstract, references, index terms

Traditional access control mechanisms rely on a reference monitor to mediate access to protected resources. Reference monitors are inherently centralized and existing attempts to distribute the functionality of the reference monitor suffer from problems of scalability.Cryptographic access control is a new distributed access control paradigm designed for a global federation of information systems. It defines an implicit access control mechanism, which relies exclusively on cryptography to provide ...

Keywords: access control, cryptography, network file systems

13 The Desert environment

Steven P. Reiss
October 1999 **ACM Transactions on Software Engineering and Methodology (TOSEM)**, Volume 8 Issue 4

Full text available: pdf(868.64 KB) Additional Information: full citation, abstract, references, citings, index terms, review

The Desert software engineering environment is a suite of tools developed to enhance programmer productivity through increased tool integration. It introduces an inexpensive form of data integration to provide additional tool capabilities and information sharing among tools, uses a common editor to give high-quality semantic feedback and to integrate different types of software artifacts, and builds virtual files on demand to address specific tasks. All this is done in an open and extensibl ...

Keywords: integrated programming environments, program editors

14 Certificate-based authorization policy in a PKI environment

Mary R. Thompson, Abdelilah Essiari, Srilekha Mudumbai
November 2003 **ACM Transactions on Information and System Security (TISSEC)**, Volume 6 Issue 4

Full text available: pdf(233.63 KB) Additional Information: full citation, abstract, references, index terms

The major emphasis of public key infrastructure has been to provide a cryptographically secure means of authenticating identities. However, procedures for authorizing the holders of these identities to perform specific actions still need additional research and development. While there are a number of proposed standards for authorization structures and protocols such as KeyNote, SPKI, and SAML based on X.509 or other key-based identities, none have been widely adopted. As part of an effort to us ...

Keywords: Public key infrastructure, XML, digital certificates

15 Scalable Networked Information Processing Environment (SNIPE)

Graham E Fagg, Keith Moore, Jack J Dongarra, Al Geist
November 1997 **Proceedings of the 1997 ACM/IEEE conference on Supercomputing (CDROM)**

Full text available: pdf(77.42 KB) Additional Information: full citation, abstract, references, citings

SNIPE is a metacomputing system that aims to provide a reliable, secure, fault-tolerant environment for long-term distributed computing applications and data stores across the global InterNet. This system combines global naming and replication of both processing and data to support large scale information processing applications leading to better availablity and reliability than currently available with typical cluster computing and/or distributed computer environments.

Keywords: MetaComputing, RCDS, SNIPE, reliable, scalable, secure

Results 1 - 15 of 15

Terms used **licens MD5**

Found **38** of **145,831**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 38

Result page: **1** 2 next

Relevance scale

1 Secret key distribution protocol using public key cryptography

Amit Parnerkar, Dennis Guster, Jayantha Herath

October 2003 **Journal of Computing Sciences in Colleges**, Volume 19 Issue 1

Full text available: pdf(74.93 KB) Additional Information: full citation, abstract, references, index terms

This paper presents the description and analysis of a protocol, which uses hybrid crypto algorithms for key distribution. A triple DES with a 168-bit key is used to generate the secret key. This secret key is transferred with the help of public key cryptography. The authentication process is accomplished by using the message digest algorithm MD5. This protocol uses mutual authentication in which, both participants have to authenticate themselves via a third trusted certificate authority (CA). Th ...

2 Technologies for repository interoperation and access control

Shirley Browne, Jack Dongarra, Jeff Horner, Paul McMahan, Scott Wells

May 1998 **Proceedings of the third ACM conference on Digital libraries**

Full text available: pdf(1.14 MB) Additional Information: full citation, references, index terms

3 Security in embedded systems: Design challenges

Srivaths Ravi, Anand Raghunathan, Paul Kocher, Sunil Hattangady

August 2004 **ACM Transactions on Embedded Computing Systems (TECS)**, Volume 3 Issue 3

Full text available: pdf(3.67 MB) Additional Information: full citation, abstract, references, index terms

Many modern electronic systems---including personal computers, PDAs, cell phones, network routers, smart cards, and networked sensors to name a few---need to access, store, manipulate, or communicate sensitive information, making security a serious concern in their design. Embedded systems, which account for a wide range of products from the electronics, semiconductor, telecommunications, and networking industries, face some of the most demanding security concerns---on the one hand, they are oft ...

Keywords: Embedded systems, architecture, authentication, battery life, cryptographic algorithms, decryption, encryption, hardware design, processing requirements, security, security attacks, security protocols, tamper resistance

4 Random oracles are practical: a paradigm for designing efficient protocols

Mihir Bellare, Phillip Rogaway

December 1993 **Proceedings of the 1st ACM conference on Computer and communications security**

Full text available: pdf(1.17 MB) Additional Information: full citation, abstract, references, citings, index terms

We argue that the random oracle model—where all parties have access to a public random oracle—provides a bridge between cryptographic theory and cryptographic practice. In the paradigm we suggest, a practical protocol P is produced by first devising and proving correct a protocol PR for the random oracle model, and then replacing oracle accesses by the computation of an "appropriately chosen" function h

5 Distributed computing
Cynthia Dwork
March 1995 **ACM SIGACT News**, Volume 26 Issue 1
Full text available: pdf(161.28 KB) Additional Information: full citation, index terms

6 Revokable and versatile electronic money (extended abstract)
Markus Jakobsson, Moti Yung
January 1996 **Proceedings of the 3rd ACM conference on Computer and communications security**
Full text available: pdf(1.53 MB) Additional Information: full citation, references, citings, index terms

7 Authentication services for computer networks and electronic messaging systems
Keok Auyong, Chye-Lin Chee
July 1997 **ACM SIGOPS Operating Systems Review**, Volume 31 Issue 3
Full text available: pdf(1.03 MB) Additional Information: full citation, abstract, index terms

The paper surveys the authentication services used by modern computer systems and presents the major operational authentication services employed by commercial companies, banking as well as government departments. As distributed system services are susceptible to a variety of threats mounted by intruders as well as legitimate users of the system, password-based authentication is not suitable for use on computer networks.

8 Session 4: Securing the download of radio configuration files for software defined radio devices
Alessandro Brawerman, Douglas Blough, Benny Bing
October 2004 **Proceedings of the second international workshop on Mobility management & wireless access protocols**
Full text available: pdf(150.74 KB) Additional Information: full citation, abstract, references, index terms

Radio configuration (R-CFG) files for software defined radio (SDR) devices can be downloaded over the air, allowing these devices to support multi-mode functionality using a single transceiver. SDR device manufacturers are likely to provide the R-CFGs, which may contain proprietary information. In such cases, it is necessary to secure the server/SDR device connection during the R-CFG download. Therefore, a protocol to securely connect manufacturer's server and SDR devices, called LSSL, is propos ...

Keywords: analysis of protocols, radio configuration, security and privacy issues and software

9 Deployment and testbeds: Enhancement of a WLAN-based internet service in Korea
Youngkyu Choi, Jeongyeup Paek, Sunghyun Choi, Go Woon Lee, Jae Hwan Lee, Hanwook Jung
September 2003 **Proceedings of the 1st ACM international workshop on Wireless mobile applications and services on WLAN hotspots**
Full text available: pdf(774.23 KB) Additional Information: full citation, abstract, references, index terms

A wireless LAN (WLAN)-based Internet service, called NESPOT, of Korea Telecom (KT), the biggest telecommunication and Internet service company in Korea, has been operational since early 2002. As the numbers of subscribers and deployed access points (APs) increase, KT has been endeavoring to improve its service quality as well as the network management. In this paper, we introduce a joint effort between Seoul National University (SNU) and KT to achieve it. We have been addressing two major issues ...

Keywords: IEEE 802.11, LAN, hotspot service, wireless internet service provider (WISP)

10 Letters
CORPORATE Linux Journal Staff
May 2002 **Linux Journal**, Volume 2002 Issue 97
Full text available: html(9.24 KB) Additional Information: full citation, index terms

11 Access control and signatures via quorum secret sharing
Moni Naor, Avishai Wool
January 1996 **Proceedings of the 3rd ACM conference on Computer and communications security**
Full text available: pdf(1.55 MB) Additional Information: full citation, references, citings, index terms

12 NetNews: Whither Windows?
Dennis Fowler
June 1998 **netWorker**, Volume 2 Issue 3
Full text available: pdf(126.28 KB) Additional Information: full citation, index terms

13 A holistic approach to high-performance computing: xgrid experience
David Przybyla, Karissa Miller, Mahmoud Pegah
October 2004 **Proceedings of the 32nd annual ACM SIGUCCS conference on User services**
Full text available: pdf(205.83 KB) Additional Information: full citation, abstract, references, index terms

The Ringling School of Art and Design is a fully accredited four-year college of visual arts and design. With a student to computer ratio of better than 2-to-1, the Ringling School has achieved national recognition for its large-scale integration of technology into collegiate visual art and design education. We have found that Mac OS X is the best operating system to train future artists and designers. Moreover, we can now buy Macs to run high-end graphics, nonlinear video editing, animation, ...

Keywords: Macintosh OS X, cluster, grid computing, high-performance computing, rendering, rendezvous, xgrid

14 Publicly detectable techniques for the protection virtual components
Gang Qu
June 2001 **Proceedings of the 38th conference on Design automation**
Full text available: pdf(131.89 KB) Additional Information: full citation, abstract, references, citings, index terms

Highlighted with the newly released intellectual property (IP) protection white paper by VSI Alliance, the protection of virtual components (VCs) has received a large amount of attention recently. Digital signature is one of the most promising solutions among the known protection mechanisms. However, the trade-off between hard-to-attack and easy-to-detect and the lack of efficient detection schemes are the major obstacles for digital signatures to thrive. In this paper, we propose a new wat ...

15 Reuse library interoperability and the World Wide Web
Shirley V. Browne, James W. Moore
May 1997 **ACM SIGSOFT Software Engineering Notes , Proceedings of the 1997 symposium on Software reusability**, Volume 22 Issue 3
Full text available: Additional Information:

pdf(1.16 MB) full citation, references, citings, index terms

16 Reuse library interoperability and the World Wide Web
Shirley V. Browne, James W. Moore
May 1997 **Proceedings of the 19th international conference on Software engineering**
Full text available: pdf(1.29 MB) Additional Information: full citation, references, index terms

17 A security architecture for fault-tolerant systems
Michael K. Reiter, Kenneth P. Birman, Robbert van Renesse
November 1994 **ACM Transactions on Computer Systems (TOCS)**, Volume 12 Issue 4
Full text available: pdf(2.50 MB) Additional Information: full citation, abstract, references, citings, index terms, review

Process groups are a common abstraction for fault-tolerant computing in distributed systems. We present a security architecture that extends the process group into a security abstraction. Integral parts of this architecture are services that securely and fault tolerantly support cryptographic key distribution. Using replication only when necessary, and introducing novel replication techniques when it was necessary, we have constructed these services both to be easily defensible against atta ...

Keywords: key distribution, multicast, process groups

18 Customized information extraction as a basis for resource discovery
Darren R. Hardy, Michael F. Schwartz
May 1996 **ACM Transactions on Computer Systems (TOCS)**, Volume 14 Issue 2
Full text available: pdf(1.91 MB) Additional Information: full citation, abstract, references, index terms, review

Indexing file contents is a powerful means of helping users locate documents, software, and other types of data among large repositories. In environments that contain many different types of data, content indexing requires type-specific processing to extract information effectively. We present a model for type-specific, user-customizable information extraction, and a system implementation called Essence. This software structure allows users to associate specialized extracti ...

Keywords: Internet, distributed indexing, resource discovery

19 Cooking with Linux: Saucy Administration Tools
Marcel Gagne
November 2000 **Linux Journal**
Full text available: html(15.73 KB) Additional Information: full citation, references, index terms

20 The evolution of Coda
M. Satyanarayanan
May 2002 **ACM Transactions on Computer Systems (TOCS)**, Volume 20 Issue 2
Full text available: pdf(441.35 KB) Additional Information: full citation, abstract, references, citings, index terms

Failure-resilient, scalable, and secure read-write access to shared information by mobile and static users over wireless and wired networks is a fundamental computing challenge. In this article, we describe how the Coda file system has evolved to meet this challenge through the development of mechanisms for server replication, disconnected operation, adaptive use of weak connectivity, isolation-only transactions, translucent caching, and opportunistic

exploitation of hardware surrogates. For eac ...

Keywords: Adaptation, Linux, UNIX, Windows, caching, conflict resolution, continuous data access, data staging, disaster recovery, disconnected operation, failure, high availability, hoarding, intermittent networks, isolation-only transactions, low-bandwidth networks, mobile computing, optimistic replica control, server replication, translucent cache management, weakly connected operation

CiteSeer Find: [ ] Documents Citations

Searching for **PHRASE md5 function**.
Restrict to: Header Title Order by: Expected citations Hubs Usage Date Try: Google (CiteSeer) Google (Web) CSB DBLP
15 documents found. **Order: number of citations.**

Keying Hash Functions for Message Authentication - Bellare, Canetti, Krawczyk (1996) (Correct) (133 citations)
cryptographic hash functions, primarily on the **MD5 function** designed by Rivest [Ri]and more recently on
ftp.cert.dfn.de/pub/docs/crypt/bck2.ps.gz

Robust IP Watermarking Methodologies for Physical Design - Kahng, al. (1998) (Correct) (23 citations)
ingredients -namely, the cryptographic hash **function MD5**, the public-key cryptosystem RSA, and the
nexus6.cs.ucla.edu/~abk/papers/conference/c80.ps

Signature Hiding Techniques for FPGA Intellectual Property.. - Lach, al (1998) (Correct) (5 citations)
the PGP-cryptography suite, the secure hash **function MD5**, and the RSA/MIT stream cipher RC4 [8]4
www.icsl.ucla.edu/~jlach/ICCAD98.ps

Cryptanalysis of MD5 Compress - Hans Dobbertin German (1996) (Correct) (4 citations)
May 2, 1996 In 1991 the hash **function MD5** was introduced by Ron Rivest as a
www.securitytechnet.com/crypto/algorithm/../../resource/crypto/algorithm/Symmetric/dobbertin.ps

Watermarking Graph Partitioning Solutions - Wolfe, Wong, Potkonjak (Correct) (1 citation)
method we use involves the cryptographic hash **function MD5** ,the public-key cryptosystem RSA, and a
www.cs.ucla.edu/~miodrag/papers/Wolfe_DAC_01.pdf

NetBuild: Automated Installation and Use of.. - Softwarelibraries Keith.. (Correct)
in a text file named "metadata"The MD5 hash **function [MD5]** is then applied to produce hashes for both
icl.cs.utk.edu/news_pub/submissions/report.pdf

Network Working Group A. Rubin Request for Comments: 1805.. - Status Of This (Correct)
registered. AUTHOR-NAME= first m. last HASH-**FUNCTION= md5**,sha, etc.FILE-LOCATION= ftp
company, school, etc.HASH-**FUNCTION= md5**,sha, etc.DATE= date list of hashes The
www.tzi.de/~cabo/pdfrfc/rfc1805.txt.pdf

Network Working Group P. Karn Request for Comments: 2523.. - Status Of This (Correct)
Size of zero is invalid. Key-Generation-**Function "MD5** Hash" Privacy-Method "Simple Masking"
of OfferedSchemes for Scheme #2. Key-Generation-**Function "MD5** Hash" Privacy-Method "DES-CBC over Mask"
and Attributes March 1999 Key-Generation-**Function "MD5** Hash" Privacy-Method "Simple Masking"
www.tzi.de/~cabo/pdfrfc/rfc2523.txt.pdf

Unknown - (Correct)
Identifiers April 2002 2.1.2 MD5 One-way Hash **Function MD5** was developed by Ron Rivest for RSA Security.
www.tzi.de/~cabo/pdfrfc/rfc3279.txt.pdf

Network Working Group P. Karn Request for Comments: 2523.. - Is Me Mo (Correct)
Size of zero is invalid. Key-Generation-**Function "MD5** Hash" Privacy-Method "Simple Masking"
of OfferedSchemes for Scheme #2. Key-Generation-**Function "MD5** Hash" Privacy-Method "DES-CBC over Mask"
and Attributes March 1999 Key-Generation-**Function "MD5** Hash" Privacy-Method "Simple Masking"
rfc.net/rfc2523.ps

RFC2104 RFC.net Page 1 of 12 - Network Working Group (Correct)
code is based on MD5 code as described in **[MD5]Function**: hmac_md5 *void hmac_md5(text,
with any iterated cryptographic hash **function. MD5** and SHA-1 are examples of such hash
rfc.net/rfc2104.ps

Public Key Infrastructure (PKI) - Neil Johnson Njohnson (Correct)
with RSA Dr =Decryption with RSA H =Hash **function (MD5)** Public Key Infrastructure Copyright 1999,
www.isse.gmu.edu/~csis/infs762/handouts/handout7.pdf

Try your query at: Google (CiteSeer) Google (Web) CSB DBLP